Please type a plus sign (+) inside this box → [+]

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	T2147-906625
First Inventor or Application Identifier	Patrick LE QUERE
Title	Architecture of an Encryption Circuit. Implementing Various Types of Encryption Algorithms...
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, DC 20231

1. ☒ * Fee Transmittal Form *(e.g., PTO/SB/17)*
(Submit an original and a duplicate for fee processing)
2. ☒ Specification [*Total Pages* 11]
(preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. ☒ Drawing(s) *(35 U.S.C. 113)* (formal) [*Total Sheets* 1]
4. Oath or Declaration [*Total Pages* 3] Decl. + 13 att'd.
   a. ☒ Newly executed (original or copy)
   b. □ Copy from a prior application (37 C.F.R. § 1.63(d))
   (for continuation/divisional with Box 16 completed)
      i. □ DELETION OF INVENTOR(S)
      Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

5. □ Microfiche Computer Program *(Appendix)*
6. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
   a. □ Computer Readable Copy
   b. □ Paper Copy (identical to computer copy)
   c. □ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☒ Assignment Papers (cover sheet & document(s)) to Bull S.A.
8. □ 37 C.F.R.§3.73(b) Statement *(when there is an assignee)* □ Power of Attorney
9. ☒ English Translation Document *(if applicable)*
10. ☒ Information Disclosure Statement (IDS)/PTO-1449 ☒ Copies of IDS Citations
11. ☒ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
13. □ * Small Entity Statement(s) *(PTO/SB/09-12)* □ Statement filed in prior application, Status still proper and desired
14. □ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
15. ☒ Other: Verification of Translator
~~Claim for Priority~~
~~Change of Address~~

16. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*

□ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No: ________/________________

Prior application information: Examiner ______________________ *Group / Art Unit:* ________________

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

□ *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* or ☒ *Correspondence address below*

Name	Edward J. Kondracki MILES & STOCKBRIDGE P.C.				
Address	1751 Pinnacle Drive - Suite 500				
City	McLean	State	VA	Zip Code	22102-3833
Country	U.S.	Telephone	703/903-9000	Fax	703/610-8686

Name *(Print/Type)*	Edward J. Kondracki	Registration No. *(Attorney/Agent)*	20,604
Signature	Edward J Kondracki	Date	Nov. 7, 2000

Burden Hour Statement: This form is estimated to take 0 2 hours to complete Time will vary depending upon the needs of the individual case Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO. Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

PTO/SB/17 (09-00)
Approved for use through 10/31/2002. OMB 0651-0032
U S Patent and Trademark Office, U.S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL for FY 2001

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 750.00

Complete if Known	
Application Number	
Filing Date	November 7, 2000
First Named Inventor	Patrick LE QUERE
Examiner Name	
Group Art Unit	
Attorney Docket No.	T2147-906625

METHOD OF PAYMENT

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to

Deposit Account Number: 501165

Deposit Account Name: MILES & STOCKBRIDGE P.C.

☒ Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

☐ Applicant claims small entity status. See 37 CFR 1 27

2. ☒ **Payment Enclosed:**

☒ Check ☐ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	710
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 710.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		Fee Paid
Total Claims	20	-20** =	0	x		=	
Independent Claims	1	- 3** =	0	x		=	
Multiple Dependent						=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

***or number previously paid, if greater, For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for *ex parte* reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	40
146	710	246	355	Filing a submission after final rejection (37 CFR § 1 129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1 129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) ______________________

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($)40.00

SUBMITTED BY				Complete *(if applicable)*	
Name *(Print/Type)*	Edward J. Kondracki	Registration No *(Attorney/Agent)*	20,604	Telephone	703/903-9000
Signature	Edward J Kondracki			Date	Nov. 7, 2000

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement. This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO Assistant Commissioner for Patents, Washington, DC 20231

Docket: T2147-906625

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Patrick LEQUERE

Serial No.:

Filed: Concurrently Herewith

For: Architecture of an encryption Circuit Implementing Various Types of Encryption Algorithms Simultaneously Without a Loss of Performance

Examiner:

Group Art Unit:

McLean, Virginia
November 7, 2000

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Please amend the subject application, filed concurrently herewith, as indicated below:

IN THE SPECIFICATION:

On page 1, after the title and before the first paragraph on page 1, insert the following heading at the left-hand margin: --**Field of the Invention**--;

Page 1, after line 12, before the paragraph "The increased need..." insert the following heading at the left-hand margin: --**Description of Related Art**--;

Page 1, after line 22, before the paragraph "The object of the..." insert the following heading at the left-hand margin: --**Summary of the Invention**--;

Page 1, line 27, after "host" insert --computer--;

Line 27, delete "by a computing machine".

Page 2, line 3, before "making" insert --for--;

Page 2, line 4, after "and" insert --for--;

Page 2, after line 22, and before "Other advantages and ...." insert the following heading at the left-hand margin: --**<u>Brief Description of the Drawings</u>**--;

Page 2, after line 25, and before "For simplicity's sake,..." insert the following heading at the left-hand margin: --**<u>Description of the Preferred Embodiments</u>**--;

Page 7, after line 14, insert the following new paragraph:

--While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims.--

<u>IN THE CLAIMS:</u>

Please cancel Claims 1-13 in their entirety and without prejudice.

Please substitute the following claims.

15. An encryption circuit (1) for simultaneously processing various encryption algorithms, the circuit adapted to be coupled with a host computer system (HS), characterized in that the circuit comprises:

- an input/output module (2), for handling data exchanges between the host system (HS) and the circuit (1) via a dedicated bus (PCI),

- an encryption module (3) coupled with the input/output module (2) said encryption module controlling encryption and decryption operations, as well as storage of all sensitive information (1) of the circuit; and

- isolation means (4) between the input/output module (2) and the encryption module (3), for making the sensitive information stored in the encryption module (3) inaccessible to the host system (HS) and for ensuring the parallelism of the operations performed by the input/output module (2) and the encryption module (3).

16. An encryption circuit according to claim 15, characterized in that the isolation means (4) of the circuit (1) comprises a double-port memory (4).

17. An encryption circuit according to claim 15 wherein this isolation means (4) comprises a double port memory coupled between the input/output module (2) and the encryption module (3), the dual-port memory (4) being coupled to a first bus and adapted to simultaneously handle the exchange of data, commands and statuses between the input/output and encryption modules (2 and 3), and isolation between the two modules (2 and 3).

18. An encryption circuit is set forth in claim 15, characterized in that the encryption module (3) comprises:

- a first encryption sub-module (3_1), dedicated to the processing of symmetric encryption algorithms, and being coupled with the first bus of the dual port memory (4);

- a second encryption sub-module (3_2), dedicated to the processing of asymmetric encryption algorithms (40) and being coupled with the first bus of the dual-port memory (4) and including a separate internal second bus isolated from the first bus of the dual-port memory (4); and

- a CMOS memory (11) coupled with the dual-port memory (4) via the first bus of the dual-port memory containing the encryption keys.

19. An encryption circuit as set forth in claim 16, characterized in that the encryption modules (3) comprises:

- a first encryption sub-module (3_1), dedicated to the processing of symmetric encryption algorithms, and being coupled with the first bus of the dual port memory (4);

- a second encryption sub-module (3_2), dedicated to the processing of asymmetric encryption algorithms (40) and being coupled with the first bus of the dual-port memory (4) and including a separate internal second bus isolated from the first bus of the dual-port memory (4); and

- a CMOS memory (11) coupled with the dual-port memory (4) via the first bus of the dual-port memory containing the encryption keys.

20. An encryption circuit as set forth in claim 17, characterized in that the encryption module (3) comprises:

- a first encryption sub-module (3_1), dedicated to the processing of symmetric encryption algorithms, and being coupled with the first bus of the dual port memory (4);

- a second encryption sub-module (3_2), dedicated to the processing of asymmetric encryption algorithms (40) and being coupled with the first bus of the dual-port memory (4) and including a separate internal second bus isolated from the first bus of the dual-port memory (4); and

- a CMOS memory (11) coupled with the dual-port memory (4) via the first bus of the dual-port memory containing the encryption keys.

21. an encryption circuit according to claim 18, characterized in that the first encryption sub-module (3_1) comprises an encryption component (9) coupled with the dual-port memory (4) via the first bus of the memory (4), comprising various encryption automata, respectively dedicated to the processing of symmetric encryption algorithms, and in that the second encryption sub-module (3_2) comprises at least two encryption processors (10_1 and 10_2), respectively dedicated tot he processing of asymmetric encryption algorithms, coupled with the encryption module (9) via the internal second bus of the second sub-module (3_2) and a bus isolator (14) for isolating the second bus from the first bus of the dual port memory.

22. An encryption circuit according to claim 21, characterized in that the encryption processors (10_1 and 10_2) of the encryption module (30 are of the CIP type.

23. An encryption circuit according to claim 21, characterized in that one (10_1) of the two encryption processors (10_1 and 10_2) is of the CIP type, and in that the other (10_2) of the two encryption processors is of the ACE type.

24. An encryption circuit according to claim 21, characterized in that one of the two encryption processor (10_2) is of the ACE type comprising a field programmable gate array (FPGA).

25. An encryption circuit according to claim 24, characterized in that the encryption component (9) is of the SCE type.

26. An encryption circuit according to claim 25, characterized in that the encryption component (9) comprises a field programmable array (FPGA).

27. An encryption circuit according to claim 26, characterized in that the second encryption sub-module (3_2) comprises a flash memory PROM (12) and an SRAM memory (13) coupled with the second internal bus of the sub-module (3_2).

28. An encryption circuit according to claim 21, further comprising a CMOS memory (11) containing security keys and security mechanisms (15) adapted to trigger a reset mechanism of the CMOS memory (11) in case of an alarm.

29. an encryption circuit according to claim 15 characterized in that the input/output module (2) comprises:

- a microcontroller (6) having an input/output processor (6_1) and a PCI interface (6_2) integrating DMA channels responsible for executing the data transfers between the host system (HS) and the circuit (1);

- a flash memory (7) containing the code of the input/output processor (6_1) and a PCI interface (6_2) integrating DMA channels responsible for executing the data transfers between the host system (HS) and the circuit (1);

- a flash memory (7) containing the code of the input/output processor (6_1); and

- an SRAM memory (8) that receives a copy of the contents of the flash memory (7) upon startup of the input/output processor (6_1).

30. An encryption circuit according to claim 15 comprising a serial link (SL) connected to input basic keys through a secure path independent of the dedicated PCI bus, said link adapted to be controlled by the encryption module (3).

31. An encryption circuit according to claim 30, characterized in that the serial link (SL) allows downloading of proprietary algorithms into the first encryption sub-module (3_1).

32. An encryption circuit as set forth in claim 15 further including a card supporting the circuit.

33. An encryption circuit as set forth in claim 18 further including a card supporting the circuit.

34. An encryption circuit as set forth in claim 21 further including a card supporting the circuit

IN THE ABSTRACT:

Delete the present Abstract in its entirety and replace with the one attached hereto as Attachment A.

REMARKS

This Preliminary Amendment is made to eliminate informalities in the specification, claims and abstract resulting from a literal translation of the French text, to eliminate the use of multiple dependent claims, and to insert headings to conform the application to U.S. practice.

The present application is believed to be in condition for examination, which action is earnestly solicited.

Respectfully,

MILES & STOCKBRIDGE P.C.

By:
Edward J. Kondracki
Reg. No. 20,604

1751 Pinnacle Drive, Suite 500
McLean VA 22102-3833
Telephone: (703) 618-8627
#9124104 v1

ABSTRACT

An encryption circuit (1) for simultaneously processing various encryption algorithms, the circuit being capable of being coupled with a host system (HS) hosted by a computing machine. The circuit (1) comprises an input/output module (2), responsible for the data exchanges between the host system (HS) and the circuit via a dedicated bus (PCI), an encryption module (3) coupled with the input/output module (2), in charge of the encryption and decryption operations as well as the storage of all of the circuit's sensitive information; and isolation means (4) between the input/output module (2) and the encryption module (3), making the sensitive information stored in the encryption module (3) inaccessible to the host system (HS), and ensuring the parallelism of the operations performed by the input/output module (2) and the encryption module (3). The circuit is supported on a peripheral component interconnect (PCI) card. The circuit is specifically adapted to provide "hardware" protection of computer servers or stations.

Attachment A to Preliminary Amendment filed November 7, 2000 in the name of LeQuere

ARCHITECTURE OF AN ENCRYPTION CIRCUIT IMPLEMENTING VARIOUS TYPES OF ENCRYPTION ALGORITHMS SIMULTANEOUSLY WITHOUT A LOSS OF PERFORMANCE

The present invention applies to the field of encryption, and more particularly, relates to an architecture of an encryption circuit implementing various types of encryption algorithms simultaneously.

This architecture is embodied by a circuit supported by a PCI (Peripheral Component Interconnect) card, and makes it possible to implement various encryption algorithms in parallel, without a loss of performance in a machine (server or station). It also plays the role of a vault in which the secret elements (keys and certificates) required for any electronic encryption function are stored.

The increased need for performance in cryptography, combined with the need for inviolability has led the manufacturers of security systems to favor hardware solutions in the form of additional cards.

Such a card, coupled with a server, constitutes the hardware security element of the server.

There are known implementations of security architectures based on ASIC (Application Specific Integrated Circuit) components, which entail high development costs for a solution that remains inflexible, both on the manufacturer end and on the user end.

Furthermore, there is no architecture existing today that is capable of executing a set of algorithms simultaneously with a guaranteed throughput for each of them.

The object of the invention is specifically to eliminate the aforementioned drawbacks and to meet the market's new demands for security.

To this end, the subject of the invention is an architecture of an encryption circuit simultaneously processing various encryption algorithms, the circuit being capable of being coupled with a host system hosted by a computing machine.

According to the invention, the circuit comprises:

- an input/output module responsible for the data exchanges between the host system and the circuit via a PCI bus;

- an encryption module coupled with the input/output module, in charge of the encryption and decryption operations as well as the storage of all of the circuit's sensitive information; and

- isolation means between the input/output module and the encryption module, making the sensitive information stored in the encryption module inaccessible to the host system, and ensuring the parallelism of the operations performed by the input/output module and the encryption module.

The first advantage of the invention is that it allows fast execution of the principal encryption algorithms with two levels of parallelism, a first parallelism of the operations performed by the input/output module and the encryption module, and a second parallelism in the execution of the various encryption algorithms.

Another advantage of the invention is to make invisible to the host system all of the encryption resources made available to the system, and to provide protected storage for secrets such as keys and certificates. The sensitive functions of the card (algorithms and keys) are all located inside the encryption module and are inaccessible from the PCI bus.

The invention also has the advantage of enabling hardware and software implementations of various encryption algorithms to coexist without a loss of performance, while guaranteeing the throughputs of each of them.

It has the further advantage of being scalable by a choice of standard microprocessor and programmable logic technologies, as opposed to more conventional implementations based on specific circuits (ASIC). The invention makes it possible, in particular, to implement proprietary algorithms simply by modifying the code of the encryption processors or by loading a new configuration file for the encryption automata of the encryption module.

Other advantages and characteristics of the present invention will emerge through the reading of the following description, given in reference to the attached figure, which represents a block diagram of an architecture according to the invention.

For simplicity's sake, the encryption/decryption module will hereinafter be called the "encryption module."

The links between each module are all two-way links unless indicated.

The encryption circuit 1 according to the invention hinges on two main modules:

- an input/output module 2 responsible for the data exchanges between the encryption resources and a host system HS via a PCI bus; and

- an encryption module 3 in charge of the encryption and decryption operations as well as the storage of the secrets.

These two modules 2 and 3, respectively delimited by an enclosing dot-and-dash line, dialogue via a dual-port memory DPR 4 that allows the exchange of data and commands/statuses between the two modules 2 and 3.

A serial link SL controlled by the encryption module 3 also makes it possible to input the basic keys through a secure path SP independent of the normal functional path (PCI bus), thus meeting the requirement imposed by the FIPS140 standard.

This link SL is connected to the card 1 via a module EPLD 5, or "Erasable Programmable Logic Device," coupled between the input/output module 2 and the encryption module 3, that ensures logical consistency between the modules.

The input/output module 2 includes the following elements:

- a microcontroller IOP 6 primarily constituted by a processor 6_1 and by a PCI interface 6_2, integrating DMA (Direct Memory Access) channels. These are channels that are specific, or dedicated, to the processor, through which the data exchanged between the memories passes, and which are coupled with the processor without using the resources of the processor;

- a flash memory 7, which is a memory that saves the stored data without a power source and whose storage capacity is for example 512 kilobytes; and

- an SRAM memory 8, from the abbreviation for "Static Random Access Memory" which is a memory that requires a power source in order to save the data stored in the memory, and whose storage capacity is for example 2 Megabytes.

The data transfers between the encryption module 3 and the host system HS take place simultaneously with the encryption operations performed by the encryption module 3, thus making it possible to optimize the overall performance of the card 1.

The flash memory 7 contains the code of the processor of the microcontroller IOP 6.

At startup, the processor copies the contents of the flash memory 7 into the SRAM memory 8; the code being executed in this memory for better performance.

The SRAM memory 8 could also be replaced by an SDRAM (Synchronous Dynamic RAM) memory, which is a fast dynamic memory.

The microcontroller IOP 6 is capable of managing this type of memory without a loss of performance.

The choice of the microcontroller depends primarily on the desired performance objectives as well as the total power consumption of the card supporting the circuit, which is generally limited to 25 W (PCI specification).

The dual-port memory DPR 4 provides the isolation between the input/output module 2 and the encryption module 3, thus making the latter inaccessible to the host system HS.

Its storage capacity in the example described is 64 kilobytes. It temporarily stores the data that is to be encrypted or decrypted by the encryption automata of the encryption module 3.

It is divided into two areas:

- a control area, for example of 4 kilobytes, in which the microcontroller IOP 6 writes the control blocks to be sent to the automata; and

- a data area, for example of 60 kilobytes, containing the data to be processed by the automata.

The encryption module 3 includes first and second encryption sub-modules 3_1 and 3_2, respectively delimited by an enclosing broken line.

The first sub-module 3_1 includes an SCE (Symmetric Cipher Engine) component 9, dedicated to the processing of symmetric encryption algorithms, coupled with the bus of the dual-port memory 4.

The second sub-module 3_2 is dedicated to the processing of asymmetric encryption algorithms.

It is coupled with the bus of the dual-port memory 4, and includes a separate internal bus isolated from the bus of the dual-port memory 4.

It also includes:

- one or two processors CIP 10_1, 10_2, from the abbreviation for "Cipher Processor";

- a processor ACE 10_2, from the abbreviation for "Asymmetric Cipher Processor," which in a variant of embodiment replaces one of the two cipher processors CIP 10_1, 10_2;

- a CMOS memory 11, for example with a storage capacity of 256 kilobytes, backed up by a battery;

- a flash memory PROM 12, from the abbreviation for "Programmable Read-Only Memory," for example with a storage capacity of 512 kilobytes; and

- an SRAM memory 13, for example with a storage capacity of 256 kilobytes.

As illustrated in the block diagram of the figure, the SCE component 9 and the CMOS memory 11 are directly coupled with the bus of the dual-port memory DPR 4, while the processors CIP 10_1 and 10_2 and the flash 12 and SRAM 13 memories are coupled with a separate bus isolated from the bus of the dual-port memory DPR 4 by means of a bus isolator 14, also called a bus "transceiver," represented in the figure by a block with two opposing arrows.

The flash memory PROM 12 located in the bus of the processors CIP 10_1 and 10_2 contains all of the software used by the encryption module 3.

The SRAM memory 13 plays two roles:

- it enables the fast execution of the code of the processors CIP 10_1 and 10_2; the code is copied into the memory from the flash memory PROM 12 at power up;

- it also makes it possible to store the data temporarily during the execution of the algorithms.

This characteristic of the architecture guarantees the independence of the various encryption automata from one another.

The processor CIP 10_1 and the processor ACE 10_2 both access the dual-port memory DPR 4 in order to read or write the data to be encrypted, but the processing of the algorithms *per se* takes place entirely within their own memory space (internal cache and SRAM 13) without interfering with the SCE component 9.

The SCE component 9 integrates the various symmetric encryption automata (one automaton per algorithm) of the DES, RC4 or other type, as well as a random number generator, not represented.

Each automaton works independently from the others and accesses the dual-port memory DPR 4 in order to read its control block (written by the microcontroller IOP 6) and the corresponding data to be processed.

The parallelism of the processing thus performed makes it possible to guarantee an optimal throughput for each algorithm even when the automata are used simultaneously.

The only limitation on the processing is imposed by access to the dual-port memory DPR 4, which is shared by all of the automata.

The bandwidth of the data bus to this memory must therefore be greater than the sum of the throughputs of each algorithm in order not to limit their performance.

The SCE component 9 is produced using a programmable technology that is also known as FPGA, or "Field Programmable Gate Array," which is a programmable circuit or chip having a high logic gate density, which provides all of the flexibility required to implement new algorithms, including proprietary algorithms, on demand.

The configuration data for this component is contained in the flash memory PROM 12, and is loaded into the SCE component 9 at power up under the control of the processor CIP 10_1.

The processor CIP 10_1, using given programming software, implements the algorithms not implemented in the SCE component 9. It also implements asymmetric algorithms of the RSA type with or without the help of the specialized automaton·implemented by the processor ACE 10_2.

It performs the initialization of the security parameters (keys) via the serial link SL.

The utilization of a high-performance processor at this level guarantees optimal performance in the execution of the algorithms as well as great flexibility for the implementation of additional algorithms.

As a result of this processor, it is also possible to download proprietary algorithms via the serial link SL.

According to a first embodiment, two processors CIP 10_1 and 10_2 are implemented:

One of them 10_1 is required for the execution of the of the RSA algorithm; the other 10_2 implements the algorithms not yet supported by the SCE component 9.

According to a second embodiment, there is only one processor CIP 10_1 assisted by a processor ACE 10_2 that replaces one of the two processors CIP 10_1 and 10_2 of the first embodiment, and which implements, in programmable logic, the intensive calculation linked to the protocol of the RSA algorithm.

All of the required algorithms are implemented in programmable logic in automata of the SCE component 9.

This component is produced in programmable FPGA technology.

The CMOS memory 11 contains the keys and other secrets of the card 1. It is backed up by a battery and protected by various known security mechanisms SM 15 which, in case of abnormalities, translate them as an intrusion attempt and erase its contents.

These abnormalities are for example due to:

- an abnormal increase or decrease in the temperature;
- an abnormal increase or decrease in the supply voltage;
- a disencryption of the card;
- a physical intrusion attempt (on-the card end or the host system end);
- etc.

Each of the above events triggers an alarm signal that acts on the reset mechanism of the CMOS memory 11.

CLAIMS

1. Architecture of an encryption circuit (1) simultaneously processing various encryption algorithms, the circuit being capable of being coupled with a host system (HS) hosted by a computing machine, characterized in that the circuit comprises:

- an input/output module (2), responsible for the data exchanges between the host system (HS) and the circuit (1) via a dedicated bus (PCI),

- an encryption module (3) coupled with the input/output module (2), in charge of the encryption and decryption operations as well as the storage of all of the circuit's sensitive information (1); and

- isolation means (4) between the input/output module (2) and the encryption module (3), making the sensitive information stored in the encryption module (3) inaccessible to the host system (HS) and ensuring the parallelism of the operations performed by the input/output module (2) and the encryption module (3).

2. Architecture according to claim 1, characterized in that the isolation means of the circuit (1) comprises a double-port memory (4) coupled between the input/output module (2) and the encryption module (3), including its own bus and simultaneously handling the exchange of data, commands and statuses between the two modules (2 and 3), and the isolation between the two modules (2 and 3).

3. Architecture according to either of claims 1 and 2, characterized in that the encryption module (3) comprises:

- a first encryption sub-module (3_1), dedicated to the processing of symmetric encryption algorithms, coupled with the bus of the dual port memory (4);

- a second encryption sub-module (3_2), dedicated to the processing of asymmetric encryption algorithms (40) coupled with the bus of the dual-port memory (4) and including a separate internal bus isolated from the bus of the dual-port memory (4); and

- a CMOS memory (11) coupled with the dual-port memory (4) via the bus of the dual-port memory containing the encryption keys.

4. Architecture according to claim 3, characterized in that the first encryption sub-module (3_1) comprises an encryption component (9) coupled with the dual-port memory (4) via the bus of the memory (4), comprising various encryption automata, respectively dedicated to the processing of symmetric encryption algorithms, and in that the second encryption sub-module (3_2) comprises at least two encryption processors (10_1 and 10_2), respectively dedicated to the processing of asymmetric encryption algorithms, coupled with the encryption module (9) via the internal bus of the second sub-module (3_2), which is isolated from the bus of the dual port memory by a bus isolator (14).

5. Architecture according to claim 4, characterized in that both processors (10_1) and 10_2) of the encryption module (3) are of the CIP type.

6. Architecture according to claim 4, characterized in that one (10_1) of the encryption processors (10_1 and 10_2) is of the CIP type, and in that the other (10_2) is of the ACE type.

7. Architecture according to claim 4, characterized in that the encryption processor (10_2) of the ACE type is produced in programmable FPGA technology.

8. Architecture according to any of claims 4 through 7, characterized in that the encryption module (9) is of the SCE type.

9. Architecture according to claim 8, characterized in that the encryption module (9) is produced in programmable FPGA technology.

10. Architecture according to any of claims 3 through 9, characterized in that the second encryption sub-module (3_2) also comprises a flash memory PROM (12) and an SRAM memory (13) coupled with the internal bus of the sub-module (3_2).

11. Architecture according to any of claims 3 through 10, characterized in that the CMOS memory (11) is protected by security mechanisms (15) that trigger the reset mechanism of the CMOS memory (11) in case of an alarm.

12. Architecture according to any of claims 1 through 11, characterized in that the input/output module (2) comprises:

- a microcontroller (6) comprising an input/output processor (6_1) and a PCI interface (6_2) integrating DMA channels responsible for executing the data transfers between the host system (HS) and the circuit (1);
- a flash memory (7) containing the code of the input/output processor (6_1); and
- an SRAM memory (8) that receives a copy of the contents of the flash memory (7) at the startup of the input/output processor (6_1).

13. Architecture according to any of the preceding claims, comprising a serial link (SL) that makes it possible to input basic keys through a secure path independent of the PCI bus, characterized in that the link is controlled by the encryption module (3).

14. Architecture according to claim 13, characterized in that the serial link (SL) allows the downloading of proprietary algorithms into the first encryption sub-module (3_1).

ABSTRACT

Architecture of an encryption circuit (1) simultaneously processing various encryption algorithms, the circuit being capable of being coupled with a host system (HS) hosted by a computing machine. The circuit (1) comprises an input/output module (2), responsible for the data exchanges between the host system (HS) and the circuit via a dedicated bus (PCI), an encryption module (3) coupled with the input/output module (2), in charge of the encryption and decryption operations as well as the storage of all of the circuit's sensitive information; and isolation means (4) between the input/output module (2) and the encryption module (3), making the sensitive information stored in the encryption module (3) inaccessible to the host system (HS), and ensuring the parallelism of the operations performed by the input/output module (2) and the encryption module (3).

The applications specifically include the "hardware" protection of computer servers or stations.

ONE FIGURE

Docket: T2147-906625

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
: Examiner:
Patrick LEQUERE :
: Group Art Unit:
Serial No.: :
:
Filed: Concurrently Herewith :
:
For: Architecture of an encryption Circuit :
Implementing Various Types of :
Encryption Algorithms Simultaneously:
Without a Loss of Performance : McLean, Virginia
November 7, 2000

PROPOSED DRAWING CHANGES

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Applicant requests approval of the drawing correction shown in red on the attached sheet of drawing showing FIG. 1.

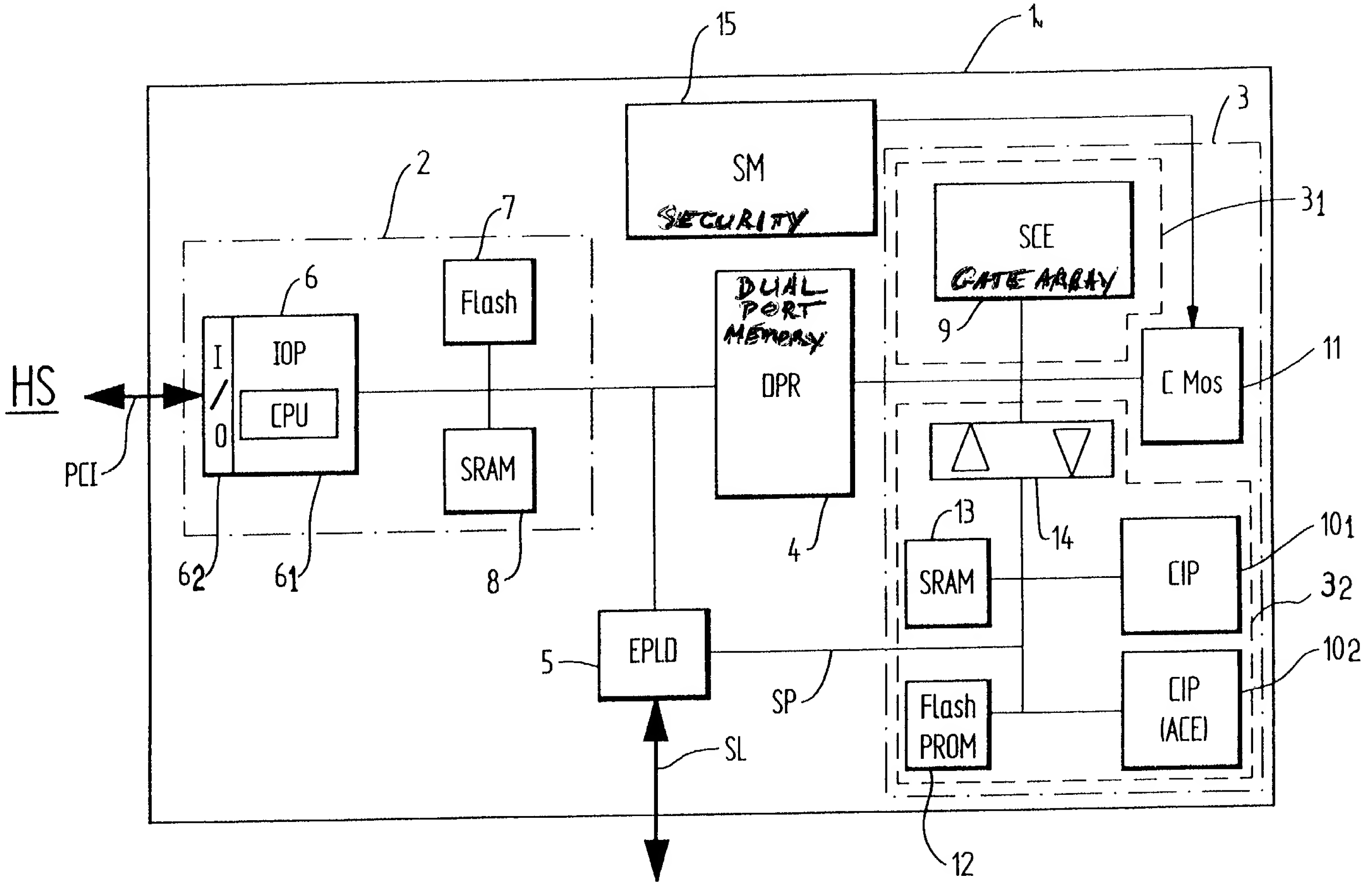
Approval is earnestly solicited.

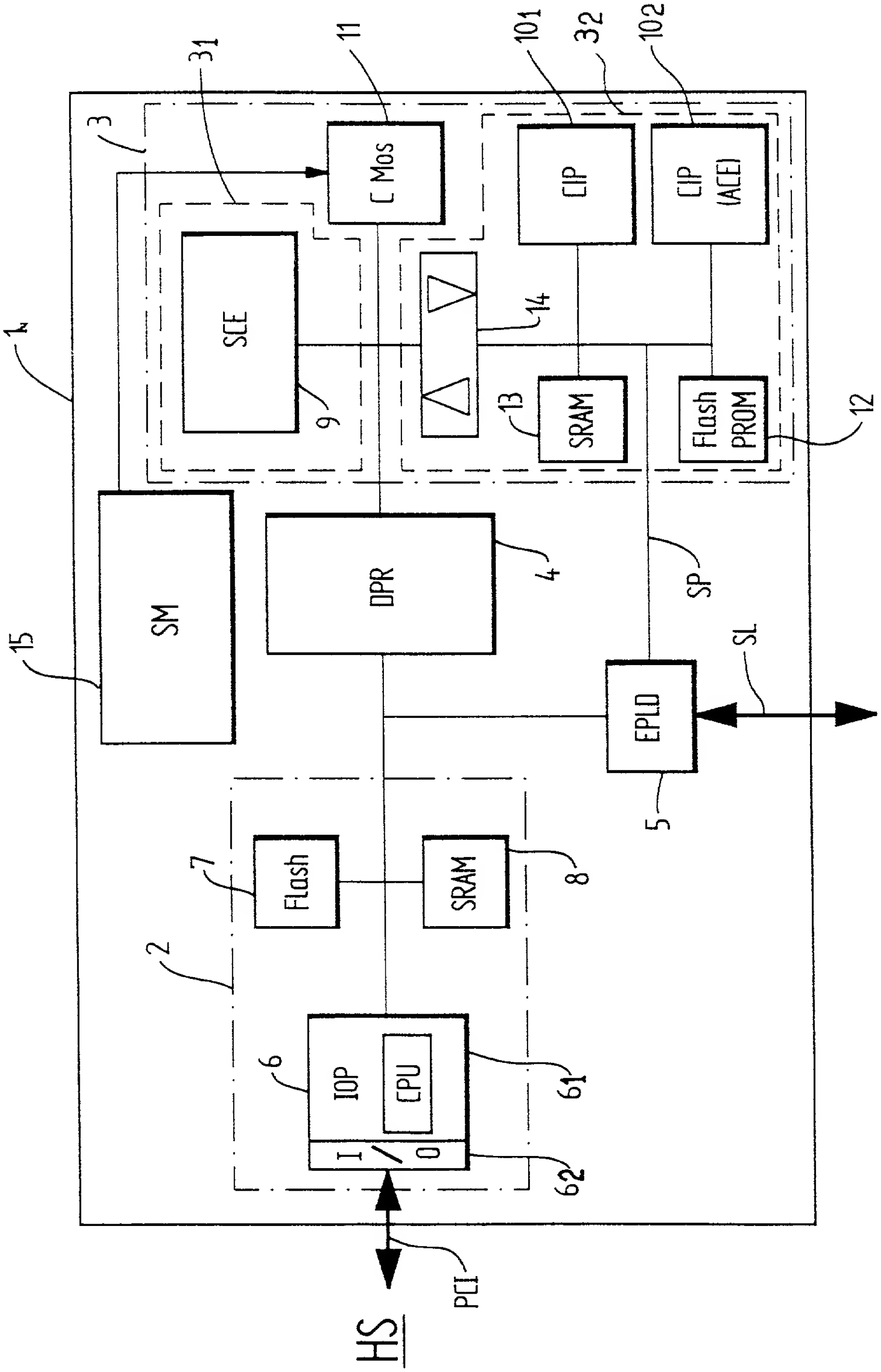
Respectfully,

MILES & STOCKBRIDGE P.C.

By:
Edward J. Kondracki
Reg. No. 20,604

1751 Pinnacle Drive, Suite 500
McLean VA 22102-3833
Telephone (703) 610-8627
#9124178 v1


HS
PCI
I/O
IOP
CPU
6
61
62
2
Flash
7
SRAM
8
SM
SECURITY
15
DUAL PORT MEMORY
DPR
4
EPLD
5
SL
SP
1
3
SCE
GATE ARRAY
9
31
C Mos
11
14
13
SRAM
CIP
101
32
CIP (ACE)
102
Flash PROM
12


1
2
3
31
32
11
101
102
C Mos
CIP
CIP (ACE)
SCE
9
14
13
SRAM
Flash PROM
12
SM
15
DPR
4
SP
SL
EPLD
5
Flash
7
SRAM
8
IOP
CPU
6
61
I / O
62
PCI
HS

Declaration and Power of Attorney For Patent Application
Declaration Pour Demandes de Brevets Avec Pouvoirs
French Language Declaration

En tant qu' inventeur nomme ci-après, Je déclare par le présent acte que:

As a below named inventor, I hereby declare that:

Mon nom, mon domicile, mon adresse postale, ma nationalité sont ceux qui figurent ci-après,

My residence, post office address and citizenship are as stated below next to my name,

Je déclare que je crois être l'inventeur original, premier et unique (si un seul nom figure sur le présent acte) ou un des co-inventeurs, originaux et premiers (si plusieurs noms figurent sur le present acte) du sujet revendiqué et pour liquel un brevet est demande sur la base de l'invention intitulée:

Architecture d'un circuit de chiffrement mettant en oeuvre différents types d'algorithmes de chiffrement simultanément sans perte de performance

dont la description
(cocher la case correspondante)

☒ est annexée au présent acte.

☐ a été déposée __________

Numéro de série de la demande __________

et modifiée le __________ (si approprié)

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

____

____

__________,

the specification of which

(check one)

☐ is attached hereto.

☐ was filed on __________ as

Application Serial No. __________

and was amended on __________. (if applicable)

Je déclare par le présent acte avoir examiné et compris le contenu de la description identifiée ci-dessus, revendications y compris, et le cas écheant telle que modifiée par l'amendment cité plus haut.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

Je reconnais le devoir de divulguer l'information qui est en rapport avec l'examen de cette demande selon Titre 37 du Code des Reglements Fédéraux §1.56(a).

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

French Language Declaration

Je revendique par le présent acte le bénéfice de priorité étrangère selon Titre 35, du Code des Etats-Unis, §119 de toute demande de brevet ou d'attestation d'inventeur énumérée ci-après, et j'ai identifié également ci-après toute demande étrangère de brevet ou d'attestation d'inventeur ayant une date de dépôt antérieure à celle de la demande pour laquelle la priorité est revendiquée.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior foreign applications

Demande(s) de brevet anteneure(s) dans un autre pays:

			Priority claimed Droit de priorité revendiqué	
FR 9914067 (Number) (Numéro)	France (Country) (Pays)	09 11 1999 (Day/Month/Year Filed) (Jour/Mois/Année de dépôt)	☒ Yes Oui	□ No Non
(Number) (Numéro)	(Country) (Pays)	(Day/Month/Year Filed) (Jour/Mois/Année de dépôt)	□ Yes Qui	□ No Non
(Number) (Numéro)	(Country) (Pays)	(Day/Month/Year Filed) (Jour/Mois/Année de dépôt)	□ Yes Oui	□ No Non

Je revendique par le présent acte, le bénéfice selon Titre 35 du Code des Etats-Unis, §120 de toute(s) demande(s) américaines énumérée(s) ci-après et, dans la mesure où le sujet de chacune des revendications de cette demande n'est pas divulgué dans la demande américaine antérieure, de la façon dêfinie par le premier paragraphe de Titre 35 du Code des Etats-Unis, §112, je reconnais le devoir de divulguer l'information pertinente selon Titre 37 du Code des Réglements Fédéraux, §1.56(a), toute information qui se présente entre la date de dépôt de la demande antérieure et la date de dépôt de la demande, soit nationale, soit internationale PCT.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.) (No. de Demande)	(Filing Date) (Date de Dépôt)	(Etat) (brevetée, pendante, abandonné)	(Status) (patented, pending, abandoned)
(Application Serial No.) (No. de Demande)	(Filing Date) (Date de Dépôt)	(Etat) (brevetée, pendante, abandonnée)	(Status) (patented, pending, abandoned)

Je déclare par le présent acte que toutes mes déclarations, à ma connaissance, sont vraies et que toutes les déclarations faites à partir de renseignements ou de suppositions, sont tenues pour être vraies; de plus, toutes ces declarations ont été faites en sachant que de fausses déclarations volontaires u autres actes de même nature sont sanctionées par une amende ou un emprisonnement, ou les deux, selon la Section 1001, du Titre 18 de Code des Etats-Unis et que de selles déclarations délibérément fausses peuvent compromettre la validité de la demande ou du brevet délivré.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

French Language Declaration

POUVOIR: En tant qu'inventeur, je désigne l'(les) avocat(s) et/ou l'(les) agent(s) suivant(s) pour poursuivre la procédure de cette demande et traiter toute affaire la concernant supris du Bureau des Brevets et de Marques:

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (*list name and registration number*)

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

Adresser toure correspondance à:

Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Send Correspondence to:

Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Adresser toute communication téléphonique à:
(*Nom*) (*Numéro de téléphone*)

Edward J. Kondracki, Esq.
(703) 998-3302

Direct Telephone Calls to: (*name and telephone number*)

Edward J. Kondracki, Esq.
(703) 998-3302

Nom complet du seul ou premier inventeur **LE QUERE Patrick**	Full name of sole or first inventor
Signature de l'inventeur Date LeQuéré 30 Novembre 1999	Inventor's signature Date
Domicile 14, allée Pierre Ronsard 91140 VILLEBON sur YVETTE FRANCE	Residence
Nationalité Française	Citizenship
Adresse Postale 14, allée Pierre Ronsard 91140 VILLEBON sur YVETTE FRANCE	Post Office Address
Nom complet du second co-inventeur, le cas echeant	Full name of second joint inventor, if any
Signature de l'inventeur Date	Second Inventor's signature Date
Domicile	Residence
Nationalité	Citizenship
Adresse Postale	Post Office Address

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)